



#13

Mayer 6-9-1
03/19/04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Mayer et al.
Case: 6-9-1
Serial No.: 09/483,876
Filing Date: January 18, 2000
Group: 2141
Examiner: Adnan M. Mirza

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: [Signature] Date: March 19, 2004

Title: Method and Apparatus for Analyzing One or More Firewalls

REQUEST TO REINSTATE APPEAL

RECEIVED

MAR 25 2004

Technology Center 2100

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Arlington, VA 22313-1450

Sir:

Applicants hereby request to reinstate the appeal. Applicants' Appeal Brief was submitted on September 17, 2003. A new Office Action was mailed on December 19, 2003.

The attention of the Examiner and the Appeal Board to this matter is appreciated.

Respectfully,

[Signature: Kevin M. Mason]

Date: March 19, 2004

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560



#14
03/30/04

Mayer 6-9-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Applicant(s): Mayer et al.
Case: 6-9-1
Serial No.: 09/483,876
Filing Date: January 18, 2000
Group: 2141
Examiner: Adnan M. Mirza

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature: *[Signature]* Date: March 19, 2004

Title: Method and Apparatus for Analyzing One or More Firewalls

SUPPLEMENTAL APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED

MAR 25 2004

Technology Center 2100

Sir:

Applicants hereby reply to the non-final Office Action, mailed December 19, 2003. A request to reinstate the appeal is submitted herewith. Applicants' Appeal Brief in an Appeal of the final rejection of claims 1 through 29 in the above-identified patent application was submitted on September 17, 2003.

REAL PARTY IN INTEREST

A statement identifying the real party in interest is contained in Applicants' Appeal Brief.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences that will directly affect or be directly affected by or have a bearing on the decision in the present appeal.

STATUS OF CLAIMS

Claims 1 through 29 are pending in the above-identified patent application. A statement identifying the original status of the claims is contained in Applicants' Appeal Brief. Claims 1 through 29 are now rejected under 35 U.S.C. §103(a) as being unpatentable over Goldberg et al. (United States Patent Number 5,146,560), Mercera et al. (United States Patent Number 5,940,252), and Flint et al. (United States Patent Number 6,453,419).

STATUS OF AMENDMENTS

A statement identifying the status of the amendments is contained in Applicants' Appeal Brief.

SUMMARY OF INVENTION

A Summary of the Invention is contained in Applicants' Appeal Brief.

ISSUES PRESENTED FOR REVIEW

A statement identifying the issues originally presented for review is contained in Applicants' Appeal Brief. In the present Office Action, the Examiner has apparently withdrawn the previous rejections and added a new rejection of claims 1-29 under 35 U.S.C. §103(a) as being unpatentable over Goldberg et al., Mercera et al., and Flint et al. Thus, the issues currently presented for review are whether claims 1-29 are properly rejected under 35 U.S.C. §103(a) as being unpatentable over Goldberg et al., Mercera et al., and Flint et al.

GROUPING OF CLAIMS

A statement identifying the grouping of the claims is contained in Applicants' Appeal Brief.

CLAIMS APPEALED

A copy of the appealed claims is contained in an Appendix of Applicants' Appeal Brief.

ARGUMENT

The Examiner is thanked for the courtesy of a telephone interview on March 16, 2004 in which the present rejection was discussed. No agreement was reached. The main point discussed with the Examiner is the difference between the definition of packet filtering rules using a graphical user interface, as taught by various prior art references, and the generation of a gateway-zone graph that models a network based on a packet filtering configuration file that includes including a plurality of such packet filtering rules, as taught and claimed by the present invention.

Applicants' original arguments are contained in Applicants' Appeal Brief and are hereby incorporated by reference. Independent Claims 1, 9, 12, 19 and 27-29 are now rejected under 35 U.S.C. §103(a) as being unpatentable over Goldberg et al., Mercera et al., and Flint et al. In particular, the Examiner acknowledges that Goldberg and Macera fail to disclose evaluating said query against each of said rules associated with each gateway node in said gateway-zone graph that is encountered between said at least one source address and said at least one destination address, but asserts that Flint discloses that "the regions that the service bridge, and the access control decisions."

The Examiner further asserts that Flint discloses that the user draws a graph which starts with service and a to-from set...The user is building a decision tree (col. 6, lines 3-11).

Applicants note that Flint teaches a graphical user interface for conveniently defining access control rules for a firewall. FIGS. 4 and 5 of Flint each illustrate an access control rule. See, e.g., col. 2, lines 48-50. In the terminology of Flint, "every access rule must consist of two specific nodes. The first, Services node 60, decides which service(s) the rule will control. The second, From/To node 62 determines the source region and destination region of the connection." Col. 4,

lines 26-31. Thus, the term “nodes” in Flint refers to nodes in a flow chart, as opposed to nodes in a network, as the term is used in the claims of the present application. The from/to node 62 of Flint identifies the source and destination regions of a given connection.

The “graphs” of Flint relied upon by the Examiner are illustrated in FIGS. 6a-6d, 7 and 8. See, e.g., Col. 2, lines 51-52. FIGS. 6a-6d show how a *single* access control rule is *built* in a graphical environment. See, col. 20, lines 30-31. FIGS. 7 and 8 each illustrate an embodiment of an access control rule. The flowcharts of FIGS. 6a-6d, 7 and 8 are created by the user to define respective access control rules. The flowchart is then used to generate the Access Control Lists (ACLs) which will be implemented by the firewall. Thus, *each graph is created by the user to input a corresponding rule to the firewall*. The Access Control Lists are used to both “restrict access to servers and to define the required filters for those services. Almost every connection to or through the firewall will use the ACL to determine whether the connection is allowed and what the conditions of the connections are.” See, col. 1, lines 27-32. The collection of ACLs generated by Flint are analogous to the “packet filtering configuration file” that is an *input* to the present invention.

Thus, each graph of Flint models an individual packet filtering rule. Independent claims 1, 12, 19, and 27 require generating a gateway-zone graph that models *said network* based on said packet filtering configuration file. Independent claims 1, 12, 19, and 27 further require that the gateway-zone graph has “at least one gateway node corresponding to said at least one gateway and at least two zone nodes.” As indicated above, the graphs of Flint only contain a Services node 60, not relevant here, and a from/to node 62 that identifies the source and destination regions of a given connection. Assuming purely for the sake of argument that the from/to node 62 can be considered “at least two zone nodes,” as required by independent claims 1, 12, 19, and 27, Flint most certainly does not teach a graph having “at least one gateway node.”

Similarly, independent claims 9 and 28-29 require generating a gateway-zone graph that models *said network* based on said packet-filtering rule-base. Again, independent claims 9 and 28-29 further require that the gateway-zone graph has “at least one gateway node corresponding to said at least one gateway and at least two zone nodes.” Assuming purely for the sake of argument that the from/to node 62 can be considered “at least two zone nodes,” as required by independent

claims 9, and 28-29, Flint most certainly does not teach a graph having “at least one gateway node.”

While Flint uses a graphical model *to generate* rules for a given firewall, the present invention generates the graphical model *from* the rules of one or more firewalls.

Thus, Goldberg, Macera, or Flint (alone or in combination) do not disclose or suggest
5 generating or analyzing a “gateway-zone graph that models said network based on said packet filtering configuration file,” as required by independent claims 1, 12, 19, and 27, and do not disclose or suggest generating a “gateway-zone graph that models said network based on said packet-filtering rule-base,” as required by independent claims 9 and 28-29.

Furthermore, Goldberg, Macera, or Flint (alone or in combination) do not disclose or
10 suggest a gateway-zone graph that has “at least one gateway node corresponding to said at least one gateway,” as well as at least two zone nodes, as required by each of the independent claims.

Conclusion

The rejections of the claims under section §103 in view of Goldberg et al., Mercera et al., and Flint et al., alone or in any combination, are therefore believed to be improper and should be
15 withdrawn.

Dependent Claims

Claims 6, 11, 16, and 24 specify a limitation providing additional bases for patentability. Specifically, the Examiner rejected claims 6, 11, 16, and 24 under 35 U.S.C. §103(a) as being unpatentable over Goldberg et al., Mercera et al., and Flint et al. Claims 6 and 24 require
20 “the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step.” Claim 11 requires “the step of transforming said packet-filtering rule-base into a table of logical rules.” Claim 16 requires “wherein said packet filtering configuration files are expressed as a set of logical rules.” The Examiner asserts that Goldberg-Macera-Flint disclosed further comprising the step of transforming said packet filtering
25 configuration files into a table of logical rules that are processed during said evaluating step (Flint: col. 5, lines 20-30).

As previously noted, Flint teaches a graphical user interface for conveniently defining rules for a firewall. The flowchart is created by the user to define the access control rules. The flowchart is then used to generate the access control commands which will be implemented by the

firewall. Thus, *the graph is created by the user to input rules to the firewall.*

Flint, in the text cited by the Examiner, discloses the steps performed “when a connection request reaches a node in a rule.” Col. 5, lines 20-30. Flint does not disclose the step of transforming packet filtering configuration files into a table of logical rules that are processed during said evaluating step.

Thus, Goldberg et al., Mercera et al., and Flint et al., alone or in combination, do not disclose or suggest “the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step,” as required by claims 6 and 24, do not disclose or suggest “the step of transforming said packet-filtering rule-base into a table of logical rules,” as required by claim 11, and do not disclose or suggest “the step of transforming said packet filtering configuration files into a table of logical rules that are processed during said evaluating step,” as required by claim 24.

The remaining rejected dependent claims are believed allowable for at least the reasons identified above with respect to the independent claims.

The attention of the Examiner and the Appeal Board to this matter is appreciated.

Respectfully submitted,



Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560

Date: March 19, 2004